22.07.2026

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Allemagne
https://www.pilz.com

Communiqué de presse

« Security for Safety » : des structures claires dans le réseau d'automatisation

Ostfildern, Allemagne, 22.07.2026 - **Andreas Willert, Head of Industrial Security auprès de Pilz Autriche**

(Seules les paroles prononcées font foi)

Le Règlement machines (UE) 2023/1230 stipule clairement que la sécurité ne peut fonctionner de manière fiable que si les fonctions de sécurité sont protégées contre la fraude. Les machines modernes sont connectées en réseau, configurées à l'aide de logiciels et ajustées pendant leur fonctionnement. Toute modification non autorisée – qu'elle soit intentionnelle ou accidentelle – peut rendre les mécanismes de protection inefficaces.

C'est pourquoi la cybersécurité n'est plus aujourd'hui un sujet secondaire, mais une condition indispensable à la sécurité. Il s'agit de garantir l'intégrité de tous les composants relatifs à la sécurité, afin que les fonctions de protection se déclenchent précisément au moment où elles sont nécessaires.

Comment les normes et les principes d'architecture garantissent une sécurité robuste
Les séries de normes IEC 62443 et la norme EN 50742, en cours d'élaboration, fournissent un cadre clair à cet égard. Les deux préconisent une architecture de sécurité systématique qui évalue les risques, met en place des mesures de protection de manière structurée et segmente clairement les systèmes.

Le principe « Zones and Conduits » est au cœur de cette approche : les systèmes sont divisés en zones, et les transitions entre celles-ci sont contrôlées. Cette approche permet une défense en profondeur (« Defence-in-Depth »), c'est-à-dire une stratégie de sécurité à plusieurs niveaux, dans laquelle plusieurs couches de protection se complètent et rendent toute fraude considérablement plus difficile.

Conformément à la norme IEC 62443, Pilz mise sur une séparation stricte entre la sécurité et l'automatisation standard. Les fonctions de sécurité sont exécutées sur du matériel distinct et sont isolées tant sur le plan organisationnel que technique. Elles restent ainsi indépendantes des mises à jour, des erreurs ou des attaques dans l'environnement standard. La surface d'attaque diminue, tout comme les efforts d'entretien.

Le degré d'isolation constitue à cet égard un facteur clé de réussite : plus les fonctions de sécurité sont isolées du réseau de production et des machines, mieux elles sont protégées. Dans le même temps, le besoin de mesures de cybersécurité supplémentaires s'en trouve réduit.

Une approche qui a fait ses preuves consiste donc à isoler les appareils qui exécutent des fonctions de sécurité dans un segment de réseau distinct. Il est essentiel de configurer correctement ce segment à l'aide de politiques d'accès et de mécanismes d'authentification supplémentaires. Les systèmes de sécurité étant très stables par rapport à l'automatisation standard et faisant rarement l'objet de modifications, cette segmentation stricte peut être facilement mise en œuvre tant du point de vue de l'efficacité que de celui de la sécurité. Il est toutefois important que les mesures définies soient systématiquement respectées tout au long du cycle de vie des machines.

C'est toutefois précisément dans le cas des machines de grande taille ou des installations complexes que la disponibilité des données de diagnostic joue un rôle important. En cas de dysfonctionnement, il est important de pouvoir déterminer rapidement pourquoi le système de sécurité s'est déclenché : un arrêt d’urgence a-t-il été actionné ? – et si oui, lequel ? Une barrière immatérielle a-t-elle été interrompue ? Et à quel endroit ? Ou y aurait-il peut-être un court-circuit dans le câblage ? Ces informations permettent de réduire considérablement les temps d'arrêt et de remettre rapidement l'installation en service. Or, les données de diagnostic ne servent pas seulement à déterminer « ce qui est en panne », mais surtout à comprendre « ce qui s'est passé exactement ».

Dans une architecture clairement segmentée, il est néanmoins possible de transmettre les données de diagnostic relatives à la sécurité à un API standard, à condition que l'accès aux fonctions de sécurité proprement dites au sein de leur zone protégée reste strictement interdit.

Pour les applications simples, les relais de sécurité de la gamme PNOZ constituent une solution adaptée, tandis que pour les machines plus complexes, une mise en œuvre sur mesure avec myPNOZ est recommandée. Ces produits ne disposent d'aucune fonctionnalité réseau et ne peuvent donc pas faire l'objet d'attaques à distance. Cela permet de réduire considérablement tant les coûts de développement que les exigences en matière de mesures de cybersécurité lors de l'exploitation. En complément, Pilz propose un programme complet de formations et de services, allant des principes fondamentaux de la cybersécurité industrielle à la certification CESA. Ces contenus expliquent comment concevoir des architectures de sécurité, évaluer les risques et améliorer durablement les mesures mises en place. C'est ainsi que l'expertise se développe exactement là où elle est nécessaire : chez ceux qui planifient, conçoivent et assument la responsabilité des systèmes.

Effets concrets de cette approche

La séparation entre la sécurité et l'automatisation standard présente de nombreux avantages tout au long du cycle de vie d'une machine :

- Sécurité renforcée : les fonctions de sécurité sont protégées contre toute modification involontaire, quoi qu'il se passe dans la zone standard.
- Moins d’efforts : les mises à jour, certifications et adaptations n'ont pas besoin d'être effectuées deux fois.
- Exploitation moins complexe : les opérateurs n’ont pas besoin de connaissances approfondies en matière de cybersécurité ; l'architecture garantit automatiquement la sécurité.
- Plus de flexibilité : les systèmes de sécurité autonomes tels que PNOZmulti 2 ou myPNOZ peuvent être intégrés quel que soit le fabricant.
- Coûts réduits : moins d'assistance, moins de licences, moins d'interventions – et donc un coût total de possession réduit.

Pilz allie une technologie robuste, des structures claires et une formation continue ciblée pour former une stratégie « Security for Safety » qui répond aux exigences normatives et facilite véritablement le quotidien : sûre, compréhensible et efficace à long terme.

Légende:

Vous trouverez des textes et des images à télécharger ci-dessous :
https://www.pilz.com/fr-INT/company/press/messages/articles/249002

Pilz – The Spirit of Safety

Pilz est un fournisseur mondial de produits, de systèmes et de prestations de services pour les techniques d'automatismes. En tant que pionnier des automatismes de sécurité, Pilz fournit la sécurité pour les personnes, les machines et l'environnement. Fondée en 1948, l'entreprise familiale dont le siège social se trouve à Ostfildern est aujourd'hui représentée dans le monde entier et compte 2 500 collaboratrices et collaborateurs répartis dans 42 filiales et succursales.
Le leader technologique propose des solutions complètes pour les automatismes concernant la sécurité et la cybersécurité industrielle des machines. Celles-ci comprennent les capteurs ainsi que les systèmes de contrôle-commande et le Motion Control – y compris les systèmes pour la communication industrielle, le diagnostic et la visualisation. Une offre internationale de prestations de services, comprenant les conseils, l'ingénierie et les formations, complète la gamme. Au-delà de la construction de machines et d'installations, les solutions de Pilz sont utilisées dans de nombreux secteurs d'activités, comme par exemple l'intralogistique, l'emballage et le ferroviaire ou dans le domaine de la robotique.

Pilz sur les réseaux sociaux

Sur nos réseaux sociaux, vous trouverez des informations concernant la vie de l'entreprise et les dernières nouveautés de nos systèmes d'automatismes.

https://www.facebook.com/pilzINT

https://www.youtube.com/user/PilzINT

https://www.linkedin.com/company/pilz

https://pilz-magazine.com/en/

Interlocuteur

Martin Kurth
Presse d’entreprise et presse spécialisée
+49 711 3409 - 0
publicrelations@pilz.com

Sabine Skaletz-Karrer
Presse spécialisée
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de